Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization

Jing Huang, *Student Member, IEEE* and A. Lee Swindlehurst, *Fellow, IEEE*

Abstract

This paper studies robust transmission schemes for multiple-input single-output (MISO) wiretap channels. Both the cases of direct transmission and cooperative jamming with a helper are investigated with imperfect channel state information (CSI) for the eavesdropper links. Robust transmit covariance matrices are obtained based on worst-case secrecy rate maximization, under both individual and global power constraints. For the case of an individual power constraint, we show that the non-convex maximin optimization problem can be transformed into a quasiconvex problem that can be efficiently solved with existing methods. For a global power constraint, the joint optimization of the transmit covariance matrices and power allocation between the source and the helper is studied via geometric programming. We also study the robust wiretap transmission problem for the case with a quality-of-service constraint at the legitimate receiver. Numerical results show the advantage of the proposed robust design. In particular, for the global power constraint scenario, although cooperative jamming is not necessary for optimal transmission with perfect eavesdropper's CSI, we show that robust jamming support can increase the worst-case secrecy rate and lower the signal to interference-plus-noise ratio at Eve in the presence of channel mismatches between the transmitters and the eavesdropper.

Index Terms

Robust beamforming, physical layer security, cooperative jamming, convex optimization.

I. INTRODUCTION

Secure transmission in wireless networks is required in many applications. Traditionally, security is considered as an issue addressed above the physical (PHY) layer, and conventional approaches for ensuring confidentially are usually based on cryptographic methods. However, the broadcast nature of wireless transmission and the dynamic topology of mobile networks may introduce significant challenges to secret key transmission and management [1], [2]. Therefore, there has recently been considerable interest from an information-theoretic perspective in the use of physical layer mechanisms to improve the security of wireless transmissions.

The theoretical basis of this area was initiated by Wyner, who introduced and studied the wiretap channel where the eavesdropper's received signal is a degraded version of the legitimate receiver's signal [3]. The secrecy capacity was defined as the upper bound of all achievable secrecy rates, which guarantee that private messages can be reliably transmitted to the receiver and kept perfectly secret from the eavesdropper. Csiszár and Körner studied a more general non-degraded wiretap channel and considered transmission of secret messages over broadcast channels [4]. Recently, considerable research has investigated secrecy in wiretap channels with multiple antennas [5]–[13]. The secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been fully characterized in [8] and [11]. In particular, for multiple-input single-output (MISO) wiretap cannels, the optimal transmit covariance matrix was found to be single-stream beamforming obtained via a closed-form solution [14], [15]. While research in this area usually assumes global channel state information (CSI) is available at the transmitter, some other work has considered the case where only partial information of the eavesdropper CSI (ECSI) is available. The optimal transmit covariance matrix that achieves the ergodic secrecy capacity for the MISO wiretap channel was studied in [16], where only statistical ECSI is assumed to be available. In [17] and [18], the problem was investigated from the perspective of maximizing the worst-case secrecy rate, where [17] considered the case that the eavesdropper's channel matrix is trace-bounded but otherwise unknown, and [18] assumed that the ECSI channel mismatch is norm-bounded.

With the additional degrees of freedom in multi-antenna or multi-node systems, many papers have considered improving the secrecy rate through the use of artificial interference [5], [13], [19], [20]. In these schemes, in addition to the information signals, part of the transmit power is allocated to jamming signals that selectively degrade the eavesdropper's channel while maintaining little interference to legitimate users. Some recent work has also considered using friendly helpers to provide jamming signals to confuse the eavesdropper [21]–[28]. This approach is often referred to as cooperative jamming.

In [21], a cooperative jamming scheme is proposed for improving the achievable secrecy sum-rate for general Gaussian multiple access and two-way relay wiretap channels. The optimal transmit weights for multiple single-antenna helpers were studied in [24], [25], where a global power constraint was imposed. A similar case with individual power constraints was studied in [27]. In [28], the optimal beamforming strategy for a cooperative jammer was studied for the MISO case under a zero-forcing constraint that nulls the interference at the legitimate receiver. However, most of the previous work on cooperative jamming assumes perfect global channel state information, including CSI for the eavesdropper. This motivates us to investigate the case when the transmitters (including helpers) have only imperfect ECSI.

In this paper, we study robust transmit precoder design for MISO wiretap channels with and without a helper. We assume that perfect CSI for the links to the legitimate user is available at both transmitters, while for the eavesdropper links there exist channel mismatches that are norm-bounded by some known constants [18], [29], [30]. Following [9], [11], [15], Gaussian inputs are assumed in the paper. We focus on obtaining robust transmit covariance matrices for 1) direct transmission (DT) without a helper and 2) cooperative jamming (CJ) schemes with a helper (friendly jammer), based on maximizing the worst-case secrecy rate. Note that our work is different from [18] in that we consider robust transmission for not only information signals but also jamming signals. We begin by studying the optimization problem under an individual power constraint, and then focus on the more complicated case with a global power constraint. For the individual power constraint case, we show that the non-convex maximin problem of maximizing the worst-case secrecy rate can be converted into a quasiconvex problem that can be efficiently solved via existing methods. For the global power constraint case, we obtain the jointly optimal transmit covariance matrices and power allocation between the source and the helper via geometric programming. In addition, following [19], [20], [31], we also consider the scenario where there is a quality-of-service (QoS) constraint at the legitimate node. In this case, we show that the introduction of the QoS constraint simplifies the optimization of the covariance and the power allocation.

The organization of the paper is as follows. Section II describes the system model considered throughout the paper. In Section III, robust design of the transmit covariance matrix is studied for the direct transmission case. The robust cooperative jamming scheme is then investigated in Section IV, where both individual and global power constraints are considered. Section V studies the case where a QoS constraint is required at the legitimate destination. The performance of the proposed robust transmission approaches are studied using several simulation examples in Section VI, and conclusions are drawn in Section VII.

The following notation is used in the paper: $\mathbb{E}\{\cdot\}$ denotes expectation, $(\cdot)^H$ the Hermitian transpose,

$|| \cdot ||$ the Euclidean norm, $(\cdot)^{\dagger}$ the pseudo-inverse, $\text{tr}(\cdot)$ is the trace operator, $\mathcal{R}(\cdot)$ represents the range space of a matrix, and $\mathbf{I}$ is an identity matrix of appropriate dimension.

II. SYSTEM MODEL

We consider a MISO communication system with a source node (Alice), a helper (Helper), a destination (Bob), and an eavesdropper (Eve). The number of antennas possessed by Alice and the Helper are denoted by N_a and N_h, respectively, while both Bob and Eve are single-antenna nodes. In this model, Alice sends private messages to Bob in the presence of Eve, who is able to eavesdrop on the link between Alice and Bob. The Helper can choose to be silent or to transmit artificial interference signals to confuse Eve. Both cases will be considered in the paper, and we refer to the former case as direct transmission (DT) and the latter as cooperative jamming (CJ). We assume that Alice and the Helper have perfect CSI for their links to Bob, but they have only imperfect CSI for their channels to Eve. We will consider cases with either individual or global power constraints.

A. Direct Transmission

When there is no support from the Helper, the received signals at Bob and Eve are given by

$$y_b = \mathbf{h}_b \mathbf{x} + n_b \tag{1a}$$

$$y_e = \mathbf{h}_e \mathbf{x} + n_e \tag{1b}$$

where $\mathbf{x}$ is the signal vector transmitted by Alice, the covariance matrix of $\mathbf{x}$ is denoted by $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$, $\text{tr}(\mathbf{Q}_x) \leq P_S$ where P_S is the transmit power constraint on Alice, and $\{\mathbf{h}_b, \mathbf{h}_e\}$ are the $1 \times N_a$ channel vectors for Bob and Eve, respectively. The terms n_b and n_e represent naturally occurring noise at Bob and Eve, and we assume that n_b and n_e are zero-mean circular complex Gaussian with variance σ_b^2 and σ_e^2. We will assume without loss of generality that $\sigma_b^2 = \sigma_e^2 = \sigma^2$.

B. Cooperative Jamming

For the case where the Helper joins the network by transmitting an i.i.d. Gaussian interference signal $\mathbf{z}$, Bob and Eve then receive

$$y_b = \mathbf{h}_b \mathbf{x} + \mathbf{g}_b \mathbf{z} + n_b \tag{2a}$$

$$y_e = \mathbf{h}_e \mathbf{x} + \mathbf{g}_e \mathbf{z} + n_e \tag{2b}$$

where we denote $\mathbf{Q}_z = \mathbb{E}\{\mathbf{z}\mathbf{z}^H\}$ and $\mathrm{tr}(\mathbf{Q}_z) \leq P_J$. The cooperative jamming optimization problems that we consider in the paper will be subject to either an individual power constraint $\mathrm{tr}(\mathbf{Q}_x) \leq P_S$, $\mathrm{tr}(\mathbf{Q}_z) \leq P_J$, or to a global power constraint $\mathrm{tr}(\mathbf{Q}_z) + \mathrm{tr}(\mathbf{Q}_z) \leq P$.

C. Channel Mismatch

For the channels between the transmitters and Eve, only estimates $\tilde{\mathbf{h}}_e$ and $\tilde{\mathbf{g}}_e$ are available at Alice and the Helper, respectively. We define the channel error vectors as

$$\mathbf{e}_h = \mathbf{h}_e - \tilde{\mathbf{h}}_e \tag{3a}$$

$$\mathbf{e}_g = \mathbf{g}_e - \tilde{\mathbf{g}}_e, \tag{3b}$$

and we assume that the channel mismatches lie in the bounded sets $\mathcal{E}_h = \{\mathbf{e}_h : ||\mathbf{e}_h||^2 \leq \epsilon_h^2\}$ and $\mathcal{E}_g = \{\mathbf{e}_g : ||\mathbf{e}_g||^2 \leq \epsilon_g^2\}$, where ϵ_h and ϵ_g are known constants. All the optimization problems in the paper are based on the $\mathbf{e}_h^* \in \mathcal{E}_h$ and $\mathbf{e}_g^* \in \mathcal{E}_g$ that give the worst performance.

III. ROBUST DIRECT TRANSMISSION

In this section, we consider the scenario where there is no jamming support from the Helper. According to the signal model (1) and (3), the secrecy rate is [9]

$$R_s = \log_2\left(1 + \frac{1}{\sigma^2}\mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H\right) - \log_2\left(1 + \frac{1}{\sigma^2}(\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e^H + \mathbf{e}_h)\right). \tag{4}$$

A power constraint is imposed such that $\mathbf{Q}_x \in \mathcal{Q}_x = \{\mathbf{Q}_x : \mathbf{Q}_x \succeq 0, \mathrm{tr}(\mathbf{Q}_x) \leq P_S\}$. For the case where perfect ECSI is available, the optimal $\mathbf{Q}_x$ has been found to be unit-rank and the corresponding beamformer is the generalized eigenvector of the matrix pencil $(\sigma^2\mathbf{I} + P_S\mathbf{h}_b^H\mathbf{h}_b, \sigma^2\mathbf{I} + P_S\mathbf{h}_e^H\mathbf{h}_e)$ corresponding to the largest generalized eigenvalue [9], [15].

We consider the case where Alice does not have perfect knowledge of the channel to Eve, but only an estimate $\tilde{\mathbf{h}}_e$. We focus on optimizing the worst-case performance, where we maximize the secrecy rate for the worst channel mismatch $\mathbf{e}_h$ in the bounded set $\mathcal{E}_h$. Therefore, the optimization problem (4) becomes

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x} \min_{\mathbf{e}_h \in \mathcal{E}_h} \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}. \tag{5}$$

The difficulty in solving this problem comes from the inner minimization over $\mathbf{e}_h$. As will be discussed later, the minimization is actually a non-convex problem. However, we will show that through a proper transformation, problem (5) can be converted to a solvable quasiconvex optimization problem.

Proposition 1: Problem (5) is equivalent to the following problem

$$\min_{\mathbf{Q}_x,\mu,\mathbf{\Psi}} \quad \frac{\sigma^2 + \mu\epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \mathbf{\Psi})\tilde{\mathbf{h}}_e^H\tilde{\mathbf{h}}_e]}{\sigma^2 + \text{tr}(\mathbf{Q}_x\mathbf{h}_b^H\mathbf{h}_b)} \tag{6a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu\mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0 \tag{6b}$$

$$\text{tr}(\mathbf{Q}_x) \leq P_S \tag{6c}$$

$$\mathbf{Q}_x \succeq 0, \mu \geq 0. \tag{6d}$$

Proof: The maximin problem in (5) can be transformed to

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, v} \quad \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{v} \tag{7a}$$

$$\text{s.t.} \quad \sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \leq v \tag{7b}$$

$$\mathbf{e}_h\mathbf{e}_h^H \leq \epsilon_h^2, \tag{7c}$$

where the constraints can also be expressed as

$$-\mathbf{e}_h\mathbf{Q}_x\mathbf{e}_h^H - 2\text{Re}(\tilde{\mathbf{h}}_e\mathbf{Q}_x\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H - \sigma^2 + v \geq 0 \tag{8}$$

$$-\mathbf{e}_h\mathbf{e}_h^H + \epsilon_h^2 \geq 0. \tag{9}$$

Using the $\mathcal{S}$-procedure [32], we know that there exists an $\mathbf{e}_h \in \mathbb{C}^{N_a}$ satisfying both the above inequalities if and only if there exists a $\mu \geq 0$ such that

$$\begin{bmatrix} \mu\mathbf{I}_{N_a} - \mathbf{Q}_x & -\mathbf{Q}_x\tilde{\mathbf{h}}_e^H \\ -\tilde{\mathbf{h}}_e\mathbf{Q}_x & -\tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H - \sigma^2 - \mu\epsilon_h^2 + v \end{bmatrix} \succeq 0. \tag{10}$$

Then we can use the property of the generalized Schur complement [33] and rewrite (10) as

$$\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x\tilde{\mathbf{h}}_e^H \leq v. \tag{11}$$

Therefore, the maximin problem in (5) becomes

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0} \quad \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x\tilde{\mathbf{h}}_e^H} \tag{12}$$

which is equivalent to

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0, \mathbf{\Psi}} \quad \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{\Psi}\tilde{\mathbf{h}}_e^H} \tag{13}$$

$$\text{s.t.} \quad \mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x \preceq \mathbf{\Psi}. \tag{14}$$

Next, we use the Schur complement to convert (14) into a linear matrix inequality (LMI), and the maximization problem is then given by

$$\min_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0, \mathbf{\Psi}} \quad \frac{\sigma^2 + \mu \epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \mathbf{\Psi})\tilde{\mathbf{h}}_e^H \tilde{\mathbf{h}}_e]}{\sigma^2 + \text{tr}(\mathbf{Q}_x \mathbf{h}_b^H \mathbf{h}_b)} \tag{15a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu \mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0, \tag{15b}$$

which completes the proof. ∎

Problem (6) consists of a linear fractional objective function, which is thus quasiconvex, with a set of LMI constraints. Therefore, we can solve this problem efficiently via the bisection method [32]. We first form the epigraph problem for (6) as

$$\min_{\mathbf{Q}_x, \mu, \mathbf{\Psi}} \quad t \tag{16a}$$

$$\text{s.t.} \quad \sigma^2 + \mu \epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \mathbf{\Psi})\tilde{\mathbf{h}}_e^H \tilde{\mathbf{h}}_e] \leq t \, [\sigma^2 + \text{tr}(\mathbf{Q}_x \mathbf{h}_b^H \mathbf{h}_b)] \tag{16b}$$

$$\begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu \mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0 \tag{16c}$$

$$\text{tr}(\mathbf{Q}_x) \leq P_S, \mathbf{Q}_x \succeq 0, \mu \geq 0, \tag{16d}$$

and the corresponding feasibility problem is then given by

$$\text{Find} \quad \mathbf{Q}_x, \mu, \mathbf{\Psi} \tag{17a}$$

$$\text{s.t.} \quad \sigma^2 + \mu \epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \mathbf{\Psi})\tilde{\mathbf{h}}_e^H \tilde{\mathbf{h}}_e] \leq t \, [\sigma^2 + \text{tr}(\mathbf{Q}_x \mathbf{h}_b^H \mathbf{h}_b)] \tag{17b}$$

$$\begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu \mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0 \tag{17c}$$

$$\text{tr}(\mathbf{Q}_x) \leq P_S, \mathbf{Q}_x \succeq 0, \mu \geq 0. \tag{17d}$$

Then we can use the following bisection method by solving the convex feasibility problem at each step until the interval that contains the optimal value converges:

Algorithm III.1: BISECTION METHOD FOR OBTAINING $\mathbf{Q}_x$

initialize: set an interval $[l, u]$ such that the optimal value $t^* \in [l, u]$, and define a tolerance $\delta > 0$.

while $u - l > \delta$

do
$\begin{cases} \textbf{let } t = (l + u)/2. \\ \text{Solve the feasibility problem in (17).} \\ \textbf{if } (17) \text{ is feasible,} \quad \textbf{then } u = t; \quad \textbf{else } l = t. \end{cases}$

For problem (6), the initial lower bound l can be chosen as any infeasible value, for example $l = \frac{\sigma^2}{\sigma^2 + P_S ||\mathbf{h}_b||^2}$, which is a lower bound since $\text{tr}(\mathbf{Q}_x \mathbf{h}_b^H \mathbf{h}_b) \leq ||\mathbf{Q}_x||_2 \cdot ||\mathbf{h}_b||^2 \leq P_S ||\mathbf{h}_b||^2$. The upper bound u can be any feasible value, for instance, we can set $u = \frac{\sigma^2 + \mu_0 \epsilon_h^2 + \text{tr}[(\mathbf{Q}_0 + \boldsymbol{\Psi}_0) \tilde{\mathbf{h}}_e^H \tilde{\mathbf{h}}_e]}{\sigma^2 + \text{tr}(\mathbf{Q}_0 \mathbf{h}_b^H \mathbf{h}_b)}$, where $\mu_0 = P_S$, $\mathbf{Q}_0 = \frac{P_S}{N_a} \mathbf{I}$, and $\boldsymbol{\Psi}_0 = \mathbf{Q}_0 (\mu_0 \mathbf{I} - \mathbf{Q}_0)^\dagger \mathbf{Q}_0$.

Note that the solution for the optimal covariance $\mathbf{Q}_x^*$ obtained from Proposition 1 is already based on a hidden worst-case channel mismatch $\mathbf{e}_h^*$. Next, we will explicitly express $\mathbf{e}_h^*$ under the norm-bounded constraint, which will be useful for the joint optimization in Section IV-B. The problem is formulated as

$$\max_{\mathbf{e}_h} \quad (\tilde{\mathbf{h}}_e + \mathbf{e}_h) \mathbf{Q}_x^* (\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \tag{18a}$$

$$\text{s.t.} \quad ||\mathbf{e}_h|| \leq \epsilon_h. \tag{18b}$$

This is a non-convex problem since we want to maximize a convex function. However, we can still obtain the global optimum by solving its dual problem, as explained in the following proposition.

Proposition 2: The worst-case channel mismatch for problem (18) is given by $\mathbf{e}_h^* = \tilde{\mathbf{h}}_e \mathbf{Q}_x^* (\lambda \mathbf{I} - \mathbf{Q}_x^*)^\dagger$, where λ is the solution of the following problem

$$\max_{\lambda \geq 0, \gamma} \quad \gamma \tag{19a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda \mathbf{I} - \mathbf{Q}_x^* & \mathbf{Q}_x^* \tilde{\mathbf{h}}_e^H \\ \tilde{\mathbf{h}}_e \mathbf{Q}_x^* & -\tilde{\mathbf{h}}_e \mathbf{Q}_x^* \tilde{\mathbf{h}}_e^H - \lambda \epsilon_h^2 - \gamma \end{bmatrix} \succeq 0. \tag{19b}$$

Proof: See Appendix A. ∎

Note that (19) is a semidefinite program (SDP) and hence can be solved efficiently using, for example, the interior-point method [32].

Thus, for the MISO wiretap channel, the problem of finding the beamformer for the worst-case eavesdropper channel can be converted from a non-convex maximin problem into a quasiconvex problem that can be solved using the bisection method. Both the optimal covariance matrix and the corresponding worst-case channel mismatch are obtained. In the following section, the MISO wiretap channel with a cooperative jammer will be investigated.

IV. ROBUST COOPERATIVE JAMMING

We now consider the case when the Helper provides cooperative jamming to improve the secrecy rate. According to the signal model in (2) and (3), the secrecy rate is

$$R_s = \log_2 \left(1 + \frac{\mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\mathbf{g}_b \mathbf{Q}_z \mathbf{g}_b^H + \sigma^2} \right) - \log_2 \left(1 + \frac{(\tilde{\mathbf{h}}_e + \mathbf{e}_h) \mathbf{Q}_x (\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}{(\tilde{\mathbf{g}}_e + \mathbf{e}_g) \mathbf{Q}_z (\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H + \sigma^2} \right). \tag{20}$$

We will first consider the optimization problem under individual power constraints, *i.e.*, $\mathbf{Q}_x \in \mathcal{Q}_x = \{\mathbf{Q}_x : \mathbf{Q}_x \succeq 0, \mathrm{tr}(\mathbf{Q}_x) \leq P_S\}$ and $\mathbf{Q}_z \in \mathcal{Q}_z = \{\mathbf{Q}_z : \mathbf{Q}_z \succeq 0, \mathrm{tr}(\mathbf{Q}_z) \leq P_J\}$, and then we investigate a more complicated case where a global power constraint $\mathrm{tr}(\mathbf{Q}_x) + \mathrm{tr}(\mathbf{Q}_z) \leq P$ is imposed.

When the ECSI is perfectly known, maximization of R_S over both $\mathbf{Q}_x$ and $\mathbf{Q}_z$ requires an iterative search [34]. However, it has also been shown that performance close to the optimal solution for the MISO wiretap channel can be obtained by simply forcing the helper's signal to be orthogonal to Bob's channel. Therefore, to simplify the solution when the ECSI is imperfect, we use a zero-forcing (ZF) constraint on the jamming signal for the CJ problem, which is equivalent to requiring that $\mathbf{Q}_z \mathbf{g}_b^H = \mathbf{0}$. With the ZF constraint, the maximization of R_S with respect to $\mathbf{Q}_z$ does not depend on $\mathbf{Q}_x$, although the optimal $\mathbf{Q}_x$ still depends on $\mathbf{Q}_z$. Thus, we will first optimize $\mathbf{Q}_z$ and then the optimal $\mathbf{Q}_x$ can be calculated.

A. Individual Power Constraint

For the case of perfect ECSI, the optimal $\mathbf{Q}_z$ under the ZF constraint is given by

$$\max_{\mathbf{Q}_z \in \mathcal{Q}_z} \quad \mathbf{g}_e \mathbf{Q}_z \mathbf{g}_e^H \tag{21a}$$

$$\text{s.t.} \quad \mathbf{g}_b \mathbf{Q}_z \mathbf{g}_b^H = 0. \tag{21b}$$

Lemma 1: The optimal covariance matrix $\mathbf{Q}_z \in \mathcal{Q}_z$ for problem (21) is rank one.

   Proof: See Appendix B. ∎

According to Lemma 1, the optimal ZF jamming signal for the perfect ECSI case is also single-stream beamforming, *i.e.* $\mathbf{Q}_z = P_J \mathbf{w} \mathbf{w}^H$, where $\mathbf{w}$ is the unit-normalized one-dimensional beamformer for the Helper. We can rewrite problem (21) as

$$\max_{\mathbf{w}} \quad |\mathbf{g}_e \mathbf{w}|^2 \tag{22a}$$

$$\text{s.t.} \quad \mathbf{g}_b \mathbf{w} = 0 \tag{22b}$$

$$\mathbf{w}^H \mathbf{w} = 1. \tag{22c}$$

The solution for problem (22) is referred to as the null-steering beamformer and is given by [35]

$$\mathbf{w}^* = \frac{(\mathbf{I}_{N_h} - \mathbf{P}_{gb})\mathbf{g}_e^H}{||(\mathbf{I}_{N_h} - \mathbf{P}_{gb})\mathbf{g}_e^H||} \tag{23}$$

where $\mathbf{P}_{gb} = \mathbf{g}_b^H(\mathbf{g}_b \mathbf{g}_b^H)^{-1}\mathbf{g}_b$ is the orthogonal projection onto the subspace spanned by $\mathbf{g}_b^H$. The optimal information covariance matrix $\mathbf{Q}_x$, similar to the perfect ECSI case discussed in Section III, is rank one and the corresponding beamformer is the generalized eigenvector of the matrix pencil $(\sigma^2 \mathbf{I} + P_S \mathbf{h}_b^H \mathbf{h}_b, \sigma_z^2 \mathbf{I} + P_S \mathbf{h}_e^H \mathbf{h}_e)$ with the largest generalized eigenvalue, where $\sigma_z^2 = \sigma^2 + \mathbf{g}_e \mathbf{Q}_z \mathbf{g}_e^H$.

For the case of imperfect ECSI, we still solve for the jamming covariance first, and the optimization problem becomes

$$\max_{\mathbf{Q}_z \in \mathcal{Q}_z} \min_{\mathbf{e}_g \in \mathcal{E}_g} \quad (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H \tag{24a}$$

$$\text{s.t.} \quad \mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H = 0. \tag{24b}$$

Proposition 3: Problem (24) is equivalent to the following problem

$$\max_{\mathbf{Q}_z, \mu, \mathbf{\Psi}} \quad \text{tr}[(\mathbf{Q}_z - \mathbf{\Psi})\tilde{\mathbf{g}}_e^H \tilde{\mathbf{g}}_e] - \mu\epsilon_g^2 \tag{25a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_z \\ \mathbf{Q}_z & \mu\mathbf{I}_{N_h} + \mathbf{Q}_z \end{bmatrix} \succeq 0 \tag{25b}$$

$$\text{tr}(\mathbf{Q}_z) \leq P_J \tag{25c}$$

$$\mathbf{Q}_z \succeq 0, \mu \geq 0 \tag{25d}$$

$$\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H = 0. \tag{25e}$$

Proof: See Appendix C. ∎

Problem (25) is an SDP that consists of a linear objective function, together with a set of LMI constraints. Therefore, we can solve this problem efficiently and obtain the optimal solution $\mathbf{Q}_z^*$. Note that although $\mathbf{e}_g$ does not explicitly appear in (25), the optimal robust covariance $\mathbf{Q}_z^*$ is already based on the hidden worst-case $\mathbf{e}_g^*$ that can be expressed explicitly through the following problem

$$\min_{\mathbf{e}_g} \quad (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z^*(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H \tag{26a}$$

$$\text{s.t.} \quad ||\mathbf{e}_g|| \leq \epsilon_g. \tag{26b}$$

This problem is similar to (18) with the difference that (26) is a convex problem and thus strong duality holds for (26) and its dual. The worst-case channel mismatch is provided through the following proposition.

Proposition 4: The worst channel mismatch for problem (26) is given by $\mathbf{e}_g^* = -\tilde{\mathbf{g}}_e\mathbf{Q}_z^*(\lambda\mathbf{I} + \mathbf{Q}_z^*)^{-1}$, where λ is the solution of the following SDP problem

$$\max_{\lambda \geq 0, \gamma} \quad \gamma \tag{27a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda\mathbf{I} + \mathbf{Q}_z^* & \mathbf{Q}_z^*\tilde{\mathbf{g}}_e^H \\ \tilde{\mathbf{g}}_e\mathbf{Q}_z^* & \tilde{\mathbf{g}}_e\mathbf{Q}_z^*\tilde{\mathbf{g}}_e^H - \lambda\epsilon_g^2 - \gamma \end{bmatrix} \succeq 0. \tag{27b}$$

Proof: See Appendix D. ∎

With solutions for $\mathbf{Q}_z^*$ and $\mathbf{e}_g^*$, we can follow (5)-(6) and formulate the optimization problem over $\mathbf{Q}_x$ as

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x} \min_{\mathbf{e}_h \in \mathcal{E}_h} \frac{\sigma^2 + (\tilde{\mathbf{g}}_e + \mathbf{e}_g^*)\mathbf{Q}_z^*(\tilde{\mathbf{g}}_e + \mathbf{e}_g^*)^H + \mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}, \tag{28}$$

which can be solved with the same procedure as in Section III.

B. Global Power Constraint

The previous sections only consider the design of the information covariance $\mathbf{Q}_x$ and the jamming covariance $\mathbf{Q}_z$ under the assumption that their individual power constraints P_S and P_J are fixed. This section investigates the joint optimization over $\mathbf{Q}_x$, $\mathbf{Q}_z$ and the power allocation between Alice and the Helper, under the constraint that $\mathrm{tr}(\mathbf{Q}_x) + \mathrm{tr}(\mathbf{Q}_z) = p_1 + p_2 \leq P$. As with the previous case, we will assume a zero-forcing constraint for the helper's jamming signal at Bob. We will first optimize the power allocation for a pair of given $\mathbf{Q}_x$ and $\mathbf{Q}_z$, and then we will provide an iterative algorithm that updates both the beamformers and the power allocation.

First, for given $\mathbf{Q}_x$ and $\mathbf{Q}_z$, let $\mathbf{Q}_x = p_1 \bar{\mathbf{Q}}_x$ and $\mathbf{Q}_z = p_2 \bar{\mathbf{Q}}_z$ where $\bar{\mathbf{Q}}_x$ and $\bar{\mathbf{Q}}_z$ are normalized such that $\mathrm{tr}(\bar{\mathbf{Q}}_x) = 1$ and $\mathrm{tr}(\bar{\mathbf{Q}}_z) = 1$. Hence the maximization of the secrecy rate (20) with respect to p_1 and p_2 is equivalent to

$$\max_{p_1, p_2 \geq 0} \quad \frac{p_1 p_2 c_1 c_3 + p_1 c_1 \sigma^2 + p_2 c_3 \sigma^2 + \sigma^4}{p_1 c_2 + p_2 c_3 + \sigma^2} \tag{29a}$$

$$\text{s.t.} \quad p_1 + p_2 \leq P \tag{29b}$$

where

$$c_1 = \mathbf{h}_b \bar{\mathbf{Q}}_x \mathbf{h}_b^H \tag{30}$$

$$c_2 = (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\bar{\mathbf{Q}}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \tag{31}$$

$$c_3 = (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\bar{\mathbf{Q}}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H. \tag{32}$$

Since (29a) is a quadratic fractional function, the optimization problem is hard to solve directly. However, we can use the *single condensation method* to solve this non-convex problem via a series of geometric programming (GP) steps [36]. GP is a class of non-linear optimization problems that can be readily turned into convex optimization problems, and hence a global optimum can be efficiently computed [37]. Before applying the single condensation method, we give the following lemma [36]:

Lemma 2: Given a posynomial

$$f(\mathbf{x}) = \sum_{i=1}^{m} u_i(\mathbf{x}) = \sum_{i=1}^{m} c_i x_1^{\beta_{1i}} x_2^{\beta_{2i}} \cdots x_n^{\beta_{ni}}, \tag{33}$$

where the exponents β_{ji} are arbitrary real numbers and c_i are positive constants, the following inequality holds:

$$f(\mathbf{x}) \geq \tilde{f}(\mathbf{x}) = \prod_{i=1}^{m} \left(\frac{u_i(\mathbf{x})}{\alpha_i} \right)^{\alpha_i}, \tag{34}$$

where $\alpha_i > 0$ and $\sum_{i=1}^{m} \alpha_i = 1$. The inequality becomes an equality when $\alpha_i = \frac{u_i(\mathbf{x_0})}{f(\mathbf{x_0})}$, in which case the monomial $\tilde{f}(\mathbf{x_0})$ is the best local approximation of the posynomial $f(\mathbf{x_0})$ near $\mathbf{x_0}$.

Proof: We can rewrite $f(\mathbf{x})$ as

$$f(\mathbf{x}) = \sum_{i=1}^{m} \alpha_i \left(\frac{u_i(\mathbf{x})}{\alpha_i} \right) \tag{35}$$

$$\geq \prod_{i=1}^{m} \left(\frac{u_i(\mathbf{x})}{\alpha_i} \right)^{\alpha_i} \tag{36}$$

where (36) holds according to the arithmetic-geometric mean inequality. When $\alpha_i = \frac{u_i(\mathbf{x_0})}{f(\mathbf{x_0})}$, we have that α_i $(i = 1, \cdots, m)$ are all positive coefficients with $\sum_{i=1}^{m} \alpha_i = 1$, and the proof of equality is straightforward by inserting α_i back into $\tilde{f}(\mathbf{x_0})$. ∎

Using Lemma 2, let

$$f(p_1, p_2) = p_1 p_2 c_1 c_3 + p_1 c_1 \sigma^2 + p_2 c_3 \sigma^2 + \sigma^4, \tag{37}$$

and rewrite the numerator of (29a) as

$$
\begin{aligned}
f(p_1, p_2) =& \tilde{f}(p_1, p_2) \\
=& \left(\frac{p_1 p_2 c_1 c_3}{\alpha_1} \right)^{\alpha_1} \left(\frac{p_1 c_1 \sigma^2}{\alpha_2} \right)^{\alpha_2} \left(\frac{p_2 c_3 \sigma^2}{\alpha_3} \right)^{\alpha_3} \left(\frac{\sigma^4}{\alpha_4} \right)^{\alpha_4}
\end{aligned} \tag{38}
$$

where

$$\alpha_1 = \frac{p_1 p_2 c_1 c_3}{f(p_1, p_2)} \tag{39}$$

$$\alpha_2 = \frac{p_1 c_1 \sigma^2}{f(p_1, p_2)} \tag{40}$$

$$\alpha_3 = \frac{p_2 c_3 \sigma^2}{f(p_1, p_2)} \tag{41}$$

$$\alpha_4 = \frac{\sigma^4}{f(p_1, p_2)}, \tag{42}$$

so the optimization problem of (29) becomes

$$\min_{p_1, p_2 \geq 0} \quad \frac{p_1 c_2 + p_2 c_3 + \sigma^2}{\tilde{f}_2(p_1, p_2)} \tag{43a}$$

$$\text{s.t.} \quad p_1 + p_2 \leq P. \tag{43b}$$

The optimization problem stated above can be readily converted into the standard form for geometric programming problems, and (43a)-(43b) are posynomials of the GP problem. Therefore, the global optimal solution can be efficiently obtained for problem (43). Next, we can use the single condensation method to solve problem (29), and the main steps are outlined in Algorithm IV.1.

Algorithm IV.1: SINGLE CONDENSATION METHOD FOR GLOBAL POWER ALLOCATION

initialize: power allocation $p_1^{(0)}$ and $p_2^{(0)}$.

iteration:

do $\begin{cases} \text{For iteration } k, \text{ evaluate posynomial } f(p_1^{(k-1)}, p_2^{(k-1)}) \text{ according to (37).} \\ \text{Compute } \alpha_i^{(k)} \text{ according to (39)-(42) using } p_1^{(k-1)}, p_2^{(k-1)}. \\ \text{Condense posynomial } f \text{ into monomial } \tilde{f} \text{ according to (38).} \\ \text{Solve problem (43) with a single GP.} \\ \text{Apply the resulting } p_1^{(k)} \text{ and } p_2^{(k)} \text{ into the first step and loop until convergence.} \end{cases}$

This successive optimization method is based on GP problems that can be solved using interior-point methods with polynomial-time complexity, and it has been proven in [36] that the solution obtained using successive approximations for the single condensation method will efficiently converge to a point satisfying the KKT conditions of the original problem.

Now we can conduct the joint optimization that considers both the information/jamming covariances and the power allocation between them. The main steps are outlined as follows:

1) Initilize $p_1 = p_2 = \frac{P}{2}$.
2) Let $P_S = p_1$, $P_J = p_2$ and solve problem (24), (28) to obtain $\mathbf{Q}_x^*$, $\mathbf{Q}_z^*$, $\mathbf{e}_h^*$ and $\mathbf{e}_g^*$.
3) Let $\bar{\mathbf{Q}}_x = \frac{\mathbf{Q}_x}{\text{tr}(\mathbf{Q}_x)}, \bar{\mathbf{Q}}_z = \frac{\mathbf{Q}_z}{\text{tr}(\mathbf{Q}_z)}$ and solve problem (29) with Algorithm IV.1.
4) Apply the resulting p_1 and p_2 to step 2 and loop until convergence.

Since in each iteration the objective functions are maximized and the secrecy rate is increased, and since there is an upper bound for the secrecy rate (the case without an eavesdropper where the jamming power is zero), the procedure will converge to an optimum. Our extensive numerical experiments, some results of which are shown in Section VI, further illustrate that the global optimum is obtained through

this procedure. Note that the non-robust counterpart of this procedure (where the CSI is assumed to be perfect) is similar but with the difference that instead of obtaining the covariance matrices from the robust maximin problems (24) and (28) in step 2, $\mathbf{Q}_x^*$ and $\mathbf{Q}_z^*$ are the solutions of the non-robust problems in (21)-(23).

V. ROBUST TRANSMIT DESIGN WITH QOS CONSTRAINT

In this section, we consider a slightly different problem in which there is a fixed constraint on the signal to interference-plus-noise ratio (SINR) of the legitimate link, so that the problem reduces to minimizing the SINR at the eavesdropper for the worst channel mismatch, under a given power constraint. As we will see, the addition of the SINR constraint actually simplifies the robust solution.

A. Robust Direct Transmission

When the Helper is silent, the optimization problem for the perfect-ECSI case is

$$\min_{\mathbf{Q}_x \in \mathcal{Q}_x} \quad \mathbf{h}_e \mathbf{Q}_x \mathbf{h}_e^H \tag{44a}$$

$$\text{s.t.} \quad \frac{\mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\sigma^2} \geq \gamma_t, \tag{44b}$$

where γ_t is the desired target SINR at Bob. When the channel mismatch is considered, the optimization problem is formulated as

$$\min_{\mathbf{Q}_x \in \mathcal{Q}_x} \max_{\mathbf{e}_h \in \mathcal{E}_h} \quad (\tilde{\mathbf{h}}_e + \mathbf{e}_h) \mathbf{Q}_x (\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \tag{45a}$$

$$\text{s.t.} \quad \frac{\mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\sigma^2} \geq \gamma_t. \tag{45b}$$

Comparing problem (45) with (5), we see that (45) simplifies the fractional expression in (5) by introducing an extra affine inequality constraint. Therefore, the procedure for solving (5) can be applied to solve (45), and we have the similar result that (45) is equivalent to the following optimization problem:

$$\min_{\mathbf{Q}_x, \mu, \mathbf{\Psi}} \quad \mu \epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \mathbf{\Psi}) \tilde{\mathbf{h}}_e^H \tilde{\mathbf{h}}_e] \tag{46a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mathbf{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu \mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0 \tag{46b}$$

$$\text{tr}(\mathbf{Q}_x) \leq P \tag{46c}$$

$$\mathbf{Q}_x \succeq 0, \mu \geq 0 \tag{46d}$$

$$\text{tr}(\mathbf{Q}_x \mathbf{h}_b^H \mathbf{h}_b) \geq \sigma^2 \gamma_t. \tag{46e}$$

Unlike the quasiconvex problem in Proposition 1 that requires a bisection method, (46) is an SDP with a linear objective function, and thus can be solved efficiently.

Note that by exploiting a similar form in (11), problem (45) is also equivalent to

$$\min_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq ||\mathbf{Q}_x||_2} \quad \mu \epsilon_h^2 + \tilde{\mathbf{h}}_e \mathbf{Q}_x \tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e \mathbf{Q}_x (\mu \mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger \mathbf{Q}_x \tilde{\mathbf{h}}_e^H \tag{47a}$$

$$\text{s.t.} \quad \frac{\mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\sigma^2} \geq \gamma_t. \tag{47b}$$

Denoting $\tilde{\mathbf{Q}}_x = \frac{\mathbf{Q}_x}{\text{tr}(\mathbf{Q}_x)}$, and based on the observation that $\tilde{\mathbf{h}}_e \mathbf{Q}_x \tilde{\mathbf{h}}_e^H \geq 0$, $\tilde{\mathbf{h}}_e \mathbf{Q}_x (\mu \mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger \mathbf{Q}_x \tilde{\mathbf{h}}_e^H \geq 0$, a relaxed solution for $\mathbf{Q}_x$ of (47) can be obtained by steering the eigenvectors of $\mathbf{Q}_x$ to maximize $\mathbf{h}_b \tilde{\mathbf{Q}}_x \mathbf{h}_b^H$ subject to a zero-forcing constraint $\tilde{\mathbf{Q}}_x \mathbf{h}_e^H = \mathbf{0}$, while allocating the eigenvalues of $\mathbf{Q}_x$ to satisfy the SINR constraint. Thus the relaxed optimization becomes

$$\max_{\tilde{\mathbf{Q}}_x} \quad \mathbf{h}_b \tilde{\mathbf{Q}}_x \mathbf{h}_b^H \tag{48a}$$

$$\text{s.t.} \quad \tilde{\mathbf{h}}_e \tilde{\mathbf{Q}}_x \tilde{\mathbf{h}}_e^H = 0, \tag{48b}$$

and $\mathbf{Q}_x^* = \frac{\sigma^2 \gamma_t}{\mathbf{h}_b \tilde{\mathbf{Q}}_x^* \mathbf{h}_b^H} \tilde{\mathbf{Q}}_x^*$. Note that (48) is also a relaxed optimization problem for its non-robust counterpart in (44), because when there is enough transmit power to meet the SINR demand, Alice will choose a beamformer that will null the signal at Eve while aligning it as close to $\mathbf{h}_b^H$ as possible. Therefore, in this case, the non-robust and robust covariance matrices, and thus the corresponding worst-case SINRs, are expected to be very close to each other. This will be illustrated by the simulation results of Section VI.

B. Robust Cooperative Jamming

Unlike the previous section, in the cooperative jamming case with a QoS constraint, we will not need to introduce a ZF constraint on the jamming signal from the helper to simplify the problem. Note also that we only consider the global power constraint scenario, since the generalization of the proposed solution to the case of individual power constraints is straightforward.

For the joint optimization of $\mathbf{Q}_x$ and $\mathbf{Q}_z$ under the QoS constraint, the optimization problem is given by

$$\min_{\mathbf{Q}_x, \mathbf{Q}_z} \max_{\mathbf{e}_h, \mathbf{e}_g} \quad \frac{(\tilde{\mathbf{h}}_e + \mathbf{e}_h) \mathbf{Q}_x (\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}{(\tilde{\mathbf{g}}_e + \mathbf{e}_g) \mathbf{Q}_z (\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H + \sigma^2} \tag{49a}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{Q}_x) + \text{tr}(\mathbf{Q}_z) \leq P \tag{49b}$$

$$|\mathbf{e}_h| \leq \epsilon_h, |\mathbf{e}_g| \leq \epsilon_g \tag{49c}$$

$$\frac{\mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H + \sigma^2} \geq \gamma_t. \tag{49d}$$

Unlike the global power allocation problem discussed in Section IV-B, the QoS constraint in problem (49) simplifies the fractional quadratic expression in (29) into a linear fractional form with respect to $\mathbf{Q}_x$ and $\mathbf{Q}_z$. Thus we can directly obtain the solution via the following proposition.

Proposition 5: Problem (49) is equivalent to the following problem

$$\min_{\mathbf{Q}_x,\mathbf{Q}_z,\boldsymbol{\Psi},\boldsymbol{\Phi},\mu,\nu} \quad \frac{\mu\epsilon_h^2 + \text{tr}[(\mathbf{Q}_x + \boldsymbol{\Psi})\tilde{\mathbf{h}}_e^H\tilde{\mathbf{h}}_e]}{\sigma^2 - \nu\epsilon_g^2 + \text{tr}[(\mathbf{Q}_z - \boldsymbol{\Phi})\tilde{\mathbf{g}}_e^H\tilde{\mathbf{g}}_e]} \tag{50a}$$

$$\text{s.t.} \quad \begin{bmatrix} \boldsymbol{\Psi} & \mathbf{Q}_x \\ \mathbf{Q}_x & \mu\mathbf{I}_{N_a} - \mathbf{Q}_x \end{bmatrix} \succeq 0 \tag{50b}$$

$$\begin{bmatrix} \boldsymbol{\Phi} & \mathbf{Q}_z \\ \mathbf{Q}_z & \nu\mathbf{I}_{N_h} + \mathbf{Q}_z \end{bmatrix} \succeq 0 \tag{50c}$$

$$\text{tr}(\mathbf{Q}_x) + \text{tr}(\mathbf{Q}_z) \leq P \tag{50d}$$

$$\mathbf{Q}_x \succeq 0, \mathbf{Q}_z \succeq 0, \mu \geq 0, \nu \geq 0 \tag{50e}$$

$$\text{tr}(\mathbf{Q}_x\mathbf{h}_b^H\mathbf{h}_b) \geq \gamma_t(\text{tr}(\mathbf{Q}_z\mathbf{g}_b^H\mathbf{g}_b) + \sigma^2). \tag{50f}$$

Proof: See Appendix E. ∎

Problem (50) is also an SDP with a quasiconvex objective function, a set of LMIs and affine inequalities. Thus it can be solved via the bisection method discussed in Section III. Note that for some cases when the SINR requirement at Bob can not be met for a given power constraint, the optimization problem will not be feasible and the transmission is assumed to be in outage. For the non-robust counterpart of the above QoS-constrained cooperative jamming problem, Alice will still use the solution of problem (44), and the Helper will use the remainder of the power for ZF jamming (same as problem (21)), since the Helper has no information about the channel mismatch.

VI. NUMERICAL RESULTS

In this section, we present some numerical examples on the secrecy rate performance of the robust transmission schemes studied in the paper. For all examples, we assume Alice and the Helper both have four antennas, *i.e.* $N_a = N_h = 4$, while Bob and Eve each has one. The channel matrices are assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. All results are calculated based on an average of 1000 independent trials. The background noise power is assumed to

be the same at Bob and Eve, $\sigma_b^2 = \sigma_e^2 = 1$, and the transmit power P is defined in dB relative to the noise power.

We will examine the performance of the robust direct transmission (DT) scheme and the robust cooperative jamming (CJ) scheme under various power constraints, channel error bounds and QoS constraints. For purposes of comparison, we also examine the non-robust generalized eigenvector schemes (which will be referred to as GEV DT) discussed in Section III , and the non-robust DT and CJ schemes discussed in Sections III-V.

Fig. 1 shows the worst-case secrecy rate as a function of transmit power under an individual power constraint, assuming $P_S = P_J$ and the channel mismatch is $\epsilon_h^2 = \epsilon_g^2 = 1.5$. In general, when there exists channel mismatch, we see that the robust design for DT and CJ produces better performance in terms of the worst-case secrecy rate compared to their non-robust counterparts. Note that the non-robust CJ scheme, although possessing twice the available power as that for DT, performs even worse than the robust DT scheme for low transmit powers. This is due to the fact that the performance of the non-robust CJ scheme is degraded not only by the channel error between Alice and Eve, but also by that between the Helper and Eve.

In Fig. 2, we compare the performance of the robust CJ scheme under both global and individual power constraints. In this case, we assume the global power limit P is 10dB, P_S and P_J are the individual power constraints for Alice and the Helper respectively, and $P_S + P_J = P$. The benefit of having the flexibility associated with a global power constraint over fixed individual power constraint is clearly evident. Also it can be seen that the proposed joint optimization procedure for the global power constraint achieves the optimal worst-case secrecy rate. When ϵ_h^2 increases, a larger fraction of the transmit power must be devoted to jamming in order to reach the higher secrecy rate.

The impact of the channel mismatch on the secrecy rate of the different schemes is presented in Fig. 3. The transmit power fraction for the robust CJ scheme is also plotted, and a global power constraint is used in this case. We assume P is 5dB, and the channel mismatch $\epsilon_h^2 = \epsilon_g^2$. It can be observed that when the channel mismatch is zero, a jamming signal is not necessary, and all schemes achieve the same secrecy rate. However, when ϵ_h^2 and ϵ_g^2 increase, the robustness of the CJ scheme is more obvious, and the jamming fraction of the total transmit power also increases. Also it can be seen that the worst-case secrecy rate is much lower for the non-robust CJ scheme due to the fact that it is impacted by the channel mismatch from both the link between Alice and Eve, and the link between the Helper and Eve.

Next, we consider examples for the case where a desired SINR constraint is imposed at Bob. P is assumed to be 10dB in these examples. In Fig. 4, the channel mismatch is given by $\epsilon_h^2 = \epsilon_g^2 = 0.5$,

and we plot the measured SINR at Bob and Eve with an increasing SINR constraint at Bob. Since the SINR constraint is met in all cases, the curves for Bob all coincide. We see that in this QoS constraint scenario, the robust CJ scheme still shows a significant performance improvement by suppressing the SINR at Eve. An interesting observation is that the robust DT scheme for minimizing the worst-case SINR at Eve shows almost the same performance as the non-robust DT method, which is consistent with the analytical prediction discussed in Section V-A. Therefore, the worst-case optimization for DT is unnecessary in this case. For the CJ schemes, when the SINR requirement at Bob is higher, more power will be allocated to Alice and less power will be used for jamming. Therefore, the performance of the CJ schemes approaches that of DT schemes.

In Fig. 5, the impact of increasing ϵ_h^2 and ϵ_g^2 is depicted. In this example, the desired SINR constraint at Bob is set to be 10dB. We see that when no channel mismatch exists, all schemes give zero SINR at Eve while maintaining the QoS constraint at Bob, and in such cases the use of artificial noise (CJ) is unnecessary. Also we can observe that although the SINR at Eve increases for all of the methods as the channel mismatch becomes larger, the benefits of using robust cooperative jamming over the other algorithms is obvious.

VII. CONCLUSIONS

In this paper, we studied robust transmit designs for MISO wiretap channels with imperfect ECSI. Robust transmit covariance matrices were obtained for both direct transmission and cooperative jamming scenarios, based on worst-case secrecy rate maximization. For the case of individual power constraints, we transformed the non-convex optimization problem into a quasiconvex problem. For the global power constraint case, we proposed an algorithm for joint optimization of the transmit covariance matrices and power allocation. In addition, we also obtained robust transmit covariance matrices for the scenario where a QoS constraint is imposed at the legitimate receiver. The benefits of the robust designs were illustrated through numerical results. We conclude that although cooperative jamming is not helpful when perfect ECSI is available under a global power constraint, the worst-case secrecy rate can be increased and the SINR at Eve can be lowered by using jamming support from a helper when the ECSI is imperfect, provided that robust beamforming is employed.

APPENDIX A

PROOF OF PROPOSITION 2

Problem (18) can be rewritten as

$$\min_{\mathbf{e}_h} \quad -\mathbf{e}_h\mathbf{Q}_x^*\mathbf{e}_h^H - 2\mathrm{Re}(\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \tag{51a}$$

$$\text{s.t.} \quad \mathbf{e}_h\mathbf{e}_h^H \leq \epsilon_h^2. \tag{51b}$$

This is a non-convex problem since its Hessian is negative semidefinite, *i.e.* $-\mathbf{Q}_x^* \preceq 0$. The Lagrangian of this problem is

$$L(\mathbf{e}_h, \lambda) = -\mathbf{e}_h\mathbf{Q}_x^*\mathbf{e}_h^H - 2\mathrm{Re}(\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H + \lambda(\mathbf{e}_h\mathbf{e}_h^H - \epsilon_h^2)$$

$$= \mathbf{e}_h(\lambda\mathbf{I} - \mathbf{Q}_x^*)\mathbf{e}_h^H + 2\mathrm{Re}(-\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 \tag{52}$$

where $\lambda \geq 0$ and the dual function is given by

$$g(\lambda) = \inf_{\mathbf{e}_h} L(\mathbf{e}_h, \lambda)$$

$$= \begin{cases} -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H & \lambda\mathbf{I} - \mathbf{Q}_x^* \succeq 0, \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \in \mathcal{R}(\lambda\mathbf{I} - \mathbf{Q}_x^*) \\ -\infty, & \text{otherwise} \end{cases} \tag{53}$$

where the unconstrained minimization of $L(\mathbf{e}_h, \lambda)$ with respect to $\mathbf{e}_h$ is achieved when $\mathbf{e}_h = \tilde{\mathbf{h}}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger$. The dual problem is thus

$$\max_{\lambda} \quad -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \tag{54a}$$

$$\text{s.t.} \quad \lambda\mathbf{I} - \mathbf{Q}_x^* \succeq 0, \ \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \in \mathcal{R}(\lambda\mathbf{I} - \mathbf{Q}_x^*). \tag{54b}$$

Using a Schur complement, the dual problem becomes the following SDP

$$\max_{\lambda \geq 0, \gamma} \quad \gamma \tag{55a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda\mathbf{I} - \mathbf{Q}_x^* & \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \\ \tilde{\mathbf{h}}_e\mathbf{Q}_x^* & -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \gamma \end{bmatrix} \succeq 0. \tag{55b}$$

Note that (51) is usually called a *trust region subproblem* (TRS), and it has been proven that strong duality holds for TRS although the objective function is non-convex [38]. Thus the optimal value of (51) and (55) are the same.

APPENDIX B

PROOF OF LEMMA 1

Since $\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H$ is nonnegative, we rewrite the equality constraint as $\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H \leq \varepsilon$, where $\varepsilon > 0$ is a arbitrarily small number. Denoting $f(\mathbf{Q}_z) = \frac{1}{\mathbf{g}_e\mathbf{Q}_z\mathbf{g}_e^H}$, the Lagrangian of problem (21) is

$$L(\mathbf{Q}_z, \lambda, \mathbf{\Theta}, \nu) = f(\mathbf{Q}_z) + \lambda(\mathrm{tr}(\mathbf{Q}_z) - P_J) - \mathrm{tr}(\mathbf{\Theta}\mathbf{Q}_z) + \nu\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H \tag{56}$$

where $\lambda \geq 0$, $\nu \geq 0$, and $\mathbf{\Theta} \succeq 0$ is the Lagrange multiplier associated with the inequality constraint $\mathbf{Q}_z \geq 0$. Note that the objective function in (21) is linear, and there exist strictly feasible points that satisfy both the inequality and equality constraints (*e.g.* $\mathbf{Q}_z = \frac{P_J}{N_h}\mathbf{w}\mathbf{w}^H$, where $\mathbf{w}$ is a normalized vector orthogonal to $\mathbf{g}_b^H$). Therefore, according to Slater's theorem, the primal and dual optimal points of (21) satisfy the Karush-Kuhn-Tucker (KKT) conditions

$$\mathrm{tr}(\mathbf{Q}_z) \leq P_J, \mathbf{Q}_z \geq 0, \mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H \leq \varepsilon \tag{57}$$

$$\lambda \geq 0, \mathbf{\Theta} \succeq 0 \tag{58}$$

$$\mathrm{tr}(\mathbf{\Theta}\mathbf{Q}_z) = 0 \tag{59}$$

$$\lambda(\mathrm{tr}(\mathbf{Q}_z) - P_J) = 0 \tag{60}$$

$$\mathbf{\Theta} = -\frac{\mathbf{g}_e^H\mathbf{g}_e}{(\mathbf{g}_e\mathbf{Q}_z\mathbf{g}_e^H)^2} + \lambda\mathbf{I} + \nu\mathbf{g}_b\mathbf{g}_b^H. \tag{61}$$

For the case that $\lambda = 0$, according to (61), we know that $\mathbf{\Theta}$ has a negative eigenvalue, which contradicts the fact that $\mathbf{\Theta}$ is positive semidefinite. Thus λ can only be positive. For $\lambda > 0$, according to (61) and since $\nu \geq 0$, $\mathbf{\Theta}$ has at least $N - 1$ positive eigenvalues, *i.e.* $\mathrm{rank}(\mathbf{\Theta}) \geq N - 1$.

Lemma 3 ([39]): Given two $N \times N$ positive semidefinite matrices $\mathbf{A}$ and $\mathbf{B}$ with eigenvalues $\lambda_i(\mathbf{A})$ and $\lambda_i(\mathbf{B})$, respectively, arranged in non-increasing order, then

$$\mathrm{tr}(\mathbf{A}\mathbf{B}) \geq \sum_{i=1}^{N} \lambda_i(\mathbf{A})\lambda_{N-i+1}(\mathbf{B}). \tag{62}$$

Combining Lemma 3 and (59), assuming $\lambda_i(\mathbf{\Theta})$ and $\lambda_i(\mathbf{Q}_z)$ are eigenvalues of $\mathbf{\Theta}$ and $\mathbf{Q}_z$, respectively, in non-increasing order, we have

$$\mathrm{tr}(\mathbf{\Theta}\mathbf{Q}_z) = 0 \geq \sum_{i=1}^{N} \lambda_i(\mathbf{\Theta})\lambda_{N-i+1}(\mathbf{Q}_z). \tag{63}$$

Due to the fact that $\mathbf{\Theta}$ and $\mathbf{Q}_z$ are both positive semidefinite matrices, we have

$$\sum_{i=1}^{N} \lambda_i(\mathbf{\Theta})\lambda_{N-i+1}(\mathbf{Q}_z) = 0. \tag{64}$$

Thus we can conclude that $\text{rank}(\boldsymbol{\Theta}) \neq N$, since otherwise all eigenvalues of $\mathbf{Q}_z$ are zero and no jamming signals are transmitted. Combining this conclusion and the above observation that $\text{rank}(\boldsymbol{\Theta}) \geq N - 1$, we can conclude that $\text{rank}(\boldsymbol{\Theta}) = N - 1$. Therefore, according to (64), we have

$$\lambda_i(\mathbf{Q}_z) \begin{cases} > 0, & i = 1 \\ = 0, & i = 2, \cdots, N, \end{cases} \tag{65}$$

which indicates that $\text{rank}(\mathbf{Q}_z) = 1$, and the proof is complete.

APPENDIX C

PROOF OF PROPOSITION 3

The proof is similar to the proof of Proposition 1. The maximin problem (24) can be transformed to

$$\max_{\mathbf{Q}_z \in \mathcal{Q}_z, v} \quad v \tag{66a}$$

$$\text{s.t.} \quad (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H \geq v \tag{66b}$$

$$\mathbf{e}_g \mathbf{e}_g^H \leq \epsilon_g^2. \tag{66c}$$

The constraints in (66) can also be expressed as

$$\mathbf{e}_g \mathbf{Q}_z \mathbf{e}_g^H + 2\text{Re}(\tilde{\mathbf{g}}_e \mathbf{Q}_z \mathbf{e}_g^H) + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - v \geq 0 \tag{67a}$$

$$- \mathbf{e}_g \mathbf{e}_g^H + \epsilon_g^2 \geq 0. \tag{67b}$$

According to the $\mathcal{S}$-procedure, there exists an $\mathbf{e}_g \in \mathbb{C}^{N_h}$ satisfying both of the above inequalities if and only if there exists a $\mu \geq 0$ such that

$$\begin{bmatrix} \mu \mathbf{I}_{N_h} + \mathbf{Q}_z & \mathbf{Q}_z \tilde{\mathbf{g}}_e^H \\ \tilde{\mathbf{g}}_e \mathbf{Q}_z & \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \mu \epsilon_g^2 - v \end{bmatrix} \succeq 0. \tag{68}$$

Applying the Schur complement, we can rewrite (68) as

$$- \mu \epsilon_g^2 + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \tilde{\mathbf{g}}_e \mathbf{Q}_z (\mu \mathbf{I}_{N_h} + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \tilde{\mathbf{g}}_e^H \geq v. \tag{69}$$

Therefore, the maximin problem (24) becomes

$$\max_{\mathbf{Q}_z \in \mathcal{Q}_z, \mu \geq 0} \quad - \mu \epsilon_g^2 + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \tilde{\mathbf{g}}_e \mathbf{Q}_z (\mu \mathbf{I}_{N_h} + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \tilde{\mathbf{g}}_e^H, \tag{70}$$

which is equivalent to

$$\max_{\mathbf{Q}_z \in \mathcal{Q}_z, \mu \geq 0, \boldsymbol{\Psi}} \quad - \mu \epsilon_g^2 + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \tilde{\mathbf{g}}_e \boldsymbol{\Psi} \tilde{\mathbf{g}}_e^H \tag{71}$$

$$\text{s.t.} \quad \mathbf{Q}_z (\mu \mathbf{I}_{N_h} + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \preceq \boldsymbol{\Psi}. \tag{72}$$

Next, we use the Schur complement to turn the above constraint into an LMI. The maximization problem is then given by

$$\max_{\mathbf{Q}_z, \mu, \boldsymbol{\Psi}} \quad -\mu \epsilon_g^2 + \text{tr}[(\mathbf{Q}_z - \boldsymbol{\Psi})\tilde{\mathbf{g}}_e^H \tilde{\mathbf{g}}_e] \tag{73a}$$

$$\text{s.t.} \quad \begin{bmatrix} \boldsymbol{\Psi} & \mathbf{Q}_z \\ \mathbf{Q}_z & \mu \mathbf{I}_{N_h} + \mathbf{Q}_z \end{bmatrix} \succeq 0 \tag{73b}$$

$$\text{tr}(\mathbf{Q}_z) \le P_J \tag{73c}$$

$$\mathbf{Q}_z \succeq 0, \mu \ge 0, \tag{73d}$$

and the proof is complete.

APPENDIX D
PROOF OF PROPOSITION 4

The proof is along the same line as that in Appendix A. Problem (26) can be rewritten as

$$\min_{\mathbf{e}_g} \quad \mathbf{e}_g \mathbf{Q}_z^* \mathbf{e}_g^H + 2\text{Re}(\tilde{\mathbf{g}}_e \mathbf{e}_g^H) + \tilde{\mathbf{g}}_e \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H \tag{74a}$$

$$\text{s.t.} \quad \mathbf{e}_g \mathbf{e}_g^H \le \epsilon_g^2, \tag{74b}$$

with the Lagrangian

$$L(\mathbf{e}_g, \lambda) = \mathbf{e}_g(\lambda \mathbf{I} + \mathbf{Q}_z^*)\mathbf{e}_g^H + 2\text{Re}(\tilde{\mathbf{g}}_e \mathbf{Q}_z^* \mathbf{e}_g^H) + \tilde{\mathbf{g}}_e \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H - \lambda \epsilon_g^2 \tag{75}$$

where $\lambda \ge 0$. It can be verified that the minimum of $L(\mathbf{e}_g, \lambda)$ with respect to $\mathbf{e}_g$ is achieved when $\mathbf{e}_g = -\tilde{\mathbf{g}}_e \mathbf{Q}_z^*(\lambda \mathbf{I} + \mathbf{Q}_z^*)^{-1}$, and hence the dual problem is

$$\max_{\lambda} \quad \tilde{\mathbf{g}}_e \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H - \lambda \epsilon_g^2 - \tilde{\mathbf{g}}_e \mathbf{Q}_z^*(\lambda \mathbf{I} + \mathbf{Q}_z^*)^{-1} \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H \tag{76a}$$

$$\text{s.t.} \quad \lambda \mathbf{I} + \mathbf{Q}_z^* \succeq 0, \ \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H \in \mathcal{R}(\lambda \mathbf{I} + \mathbf{Q}_z^*). \tag{76b}$$

Using a Schur complement, the dual problem becomes the following SDP

$$\max_{\lambda \ge 0, \gamma} \quad \gamma \tag{77a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda \mathbf{I} + \mathbf{Q}_z^* & \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H \\ \tilde{\mathbf{g}}_e \mathbf{Q}_z^* & \tilde{\mathbf{g}}_e \mathbf{Q}_z^* \tilde{\mathbf{g}}_e^H - \lambda \epsilon_g^2 - \gamma \end{bmatrix} \succeq 0, \tag{77b}$$

which completes the proof.

APPENDIX E

PROOF OF PROPOSITION 5

The maximin problem (49) can be transformed to

$$\min_{\mathbf{Q}_x \mathbf{Q}_z, v, t} \quad \frac{v}{t} \tag{78a}$$

$$\text{s.t.} \quad (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \leq v \tag{78b}$$

$$\sigma^2 + (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H \geq t \tag{78c}$$

$$\text{tr}(\mathbf{Q}_x) + \text{tr}(\mathbf{Q}_z) \leq P \tag{78d}$$

$$|\mathbf{e}_h| \leq \epsilon_h \tag{78e}$$

$$|\mathbf{e}_g| \leq \epsilon_g \tag{78f}$$

$$\mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H = \gamma_t (\mathbf{g}_b \mathbf{Q}_z \mathbf{g}_b^H + \sigma^2). \tag{78g}$$

Using the $\mathcal{S}$-procedure similarly as in (8)-(12) for (78b), (78e) and for (78c), (78f), problem (78) can be rewritten as

$$\min_{\mathbf{Q}_x, \mathbf{Q}_z, \mu \geq 0, \nu \geq 0} \quad \frac{\mu \epsilon_h^2 + \tilde{\mathbf{h}}_e \mathbf{Q}_x \tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e \mathbf{Q}_x (\mu \mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger \mathbf{Q}_x \tilde{\mathbf{h}}_e^H}{\sigma^2 - \nu \epsilon_g^2 + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \tilde{\mathbf{g}}_e \mathbf{Q}_z (\nu \mathbf{I}_{N_h} + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \tilde{\mathbf{g}}_e^H}, \tag{79}$$

which is equivalent to

$$\min_{\mathbf{Q}_x, \mathbf{Q}_z, \mu \geq 0, \nu \geq 0, \mathbf{\Psi}, \mathbf{\Phi}} \quad \frac{\mu \epsilon_h^2 + \tilde{\mathbf{h}}_e \mathbf{Q}_x \tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e \mathbf{\Psi} \tilde{\mathbf{h}}_e^H}{\sigma^2 - \nu \epsilon_g^2 + \tilde{\mathbf{g}}_e \mathbf{Q}_z \tilde{\mathbf{g}}_e^H - \tilde{\mathbf{g}}_e \mathbf{\Phi} \tilde{\mathbf{g}}_e^H} \tag{80a}$$

$$\text{s.t.} \quad \mathbf{Q}_x (\mu \mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger \mathbf{Q}_x \preceq \mathbf{\Psi} \tag{80b}$$

$$\mathbf{Q}_z (\mu \mathbf{I}_{N_h} + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \preceq \mathbf{\Phi}. \tag{80c}$$

Using the Schur complement for the above constraints, the expression in (50) can be obtained.

REFERENCES

[1] M. Debbah, "Mobile flexible networks: The challenges ahead," in *Proc. Int. Conf. Advanced Technologies for Communications (ATC)*, Oct. 2008, pp. 3–7.

[2] Y. Liang, H. V. Poor, and S. S. Shamai, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. Int. Symp. Information Theory (ISIT)*, Sep. 2005, pp. 2152–2155.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[9] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2007, pp. 2466–2470.

[10] R. Liu, R. Bustin, S. Shamai, and H. V. Poor, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2009, pp. 2602–2606.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jul. 2008, pp. 524–528.

[12] A. O. Hero III, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2007, pp. 2471–2475.

[14] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conf. Information Sciences and Systems (CISS)*, Mar. 2007, pp. 905–910.

[15] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[16] J. Li and A. P. Petropulu, "On ergodic secrecy capacity for Gaussian MISO wiretap channels," Mar. 2010. [Online]. Available: http://arxiv.org/abs/1003.2372v1

[17] A. Wolf and E. Jorswieck, "Maximization of worst-case secrecy rates in MIMO wiretap channels," in *Proc. 44th Asilomar Conference on Signals, Systems and Computers*, Nov. 2010.

[18] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM)*, Nov. 2009, pp. 1–5.

[19] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Apr. 2009, pp. 2437–2440.

[20] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[21] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[22] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[23] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. 43rd Asilomar Conference on Signals, Systems and Computers*, Nov. 2009, pp. 1719–1723.

[24] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[25] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," Jan. 2010. [Online]. Available: http://arxiv.org/abs/1001.1389

[26] J. Huang and A. L. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[27] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[28] A. Wolf and E. A. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in *Proc. IEEE Eleventh Int Signal Processing Advances in Wireless Communications (SPAWC) Workshop*, Jun. 2010, pp. 1–5.

[29] S. A. Vorobyov, A. B. Gershman, and Z.-Q. Luo, "Robust adaptive beamforming using worst-case performance optimization: A solution to the signal mismatch problem," *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 313–324, Feb. 2003.

[30] J. Wang and D. P. Palomar, "Worst-case robust MIMO transmission with imperfect channel knowledge," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086–3100, Aug. 2009.

[31] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. 10th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Jun. 2009, pp. 344–348.

[32] S. P. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge University Press, 2004.

[33] D. Carlson, E. Haynsworth, and T. Markham, "A generalization of the Schur complement by means of the Moore-Penrose inverse," *SIAM Journal on Applied Mathematics*, vol. 26, no. 1, pp. 169–175, Jan. 1974.

[34] E. A. Jorswieck, "Secrecy capacity of single- and multi-antenna channels with simple helpers," in *Proc. Int Source and Channel Coding (SCC) ITG Conf.*, Jan. 2010, pp. 1–6.

[35] B. Friedlander and B. Porat, "Performance analysis of a null-steering algorithm based on direction-of-arrival estimation," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 37, no. 4, pp. 461–466, Apr. 1989.

[36] M. Chiang, C. W. Tan, D. P. Palomar, D. O'Neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.

[37] S. Boyd, S. J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimization and Engineering*, vol. 8, no. 1, pp. 67–127, Apr. 2007.

[38] R. J. Stern and H. Wolkowicz, "Indefinite trust region subproblems and nonsymmetric eigenvalue perturbations," *SIAM Journal on Optimization*, vol. 5, no. 2, pp. 286–313, May 1995.

[39] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its Applications.* New York: Academic Press, 1979.
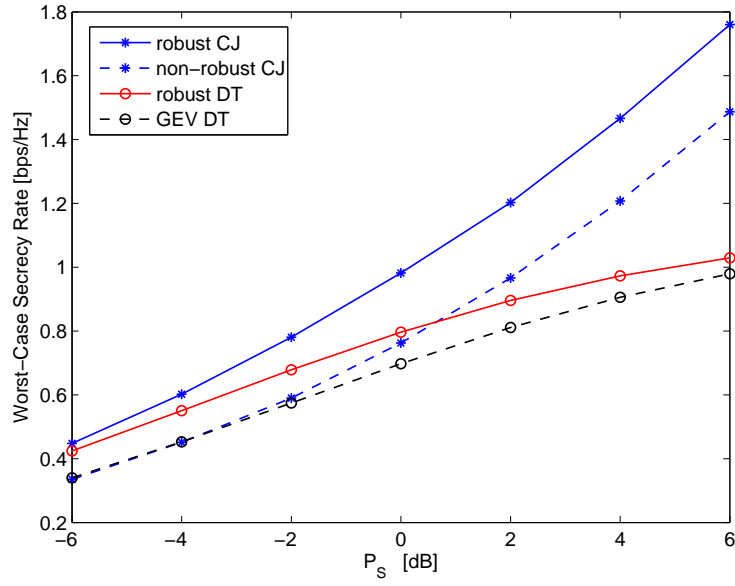
Fig. 1.   Worst-case secrecy rate vs. transmit power, with individual power constraint, $\epsilon_h^2 = \epsilon_g^2 = 1.5$.
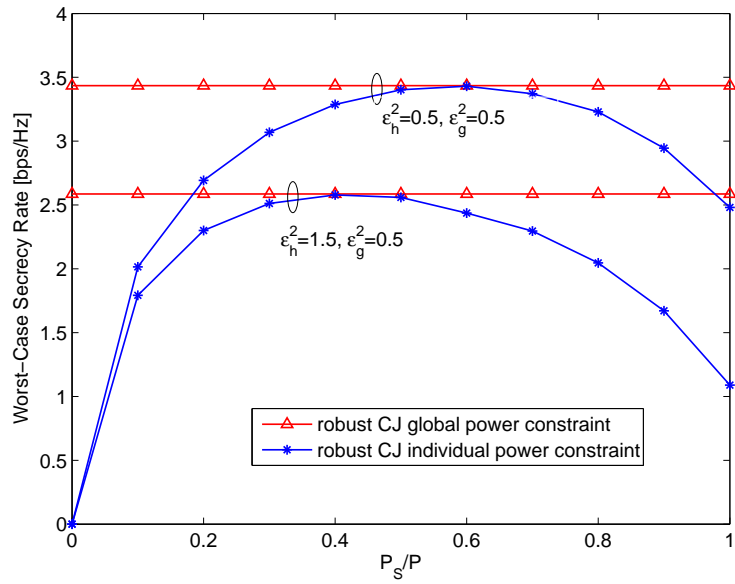

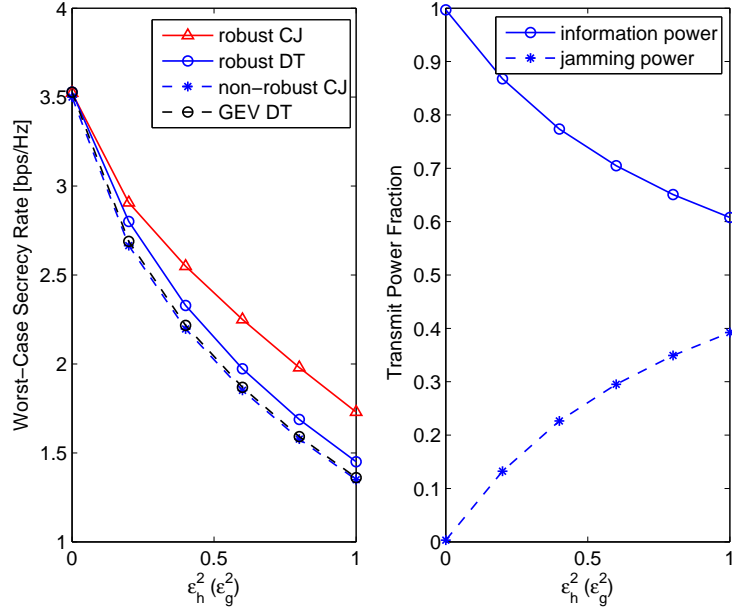Fig. 2.   Worst-case secrecy rate vs. transmit power fraction, $P = 10\text{dB}$.

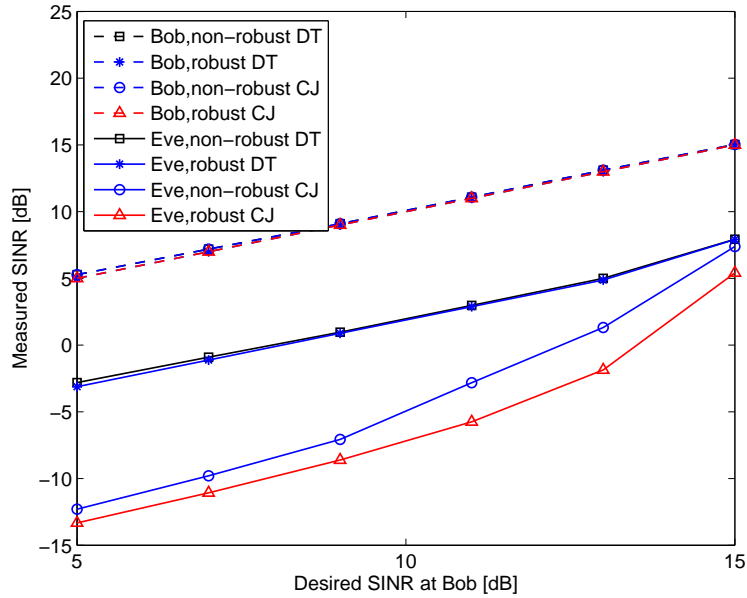Fig. 3. Worst-case secrecy rate and transmit power fraction vs. channel mismatch, $P = 5$dB.

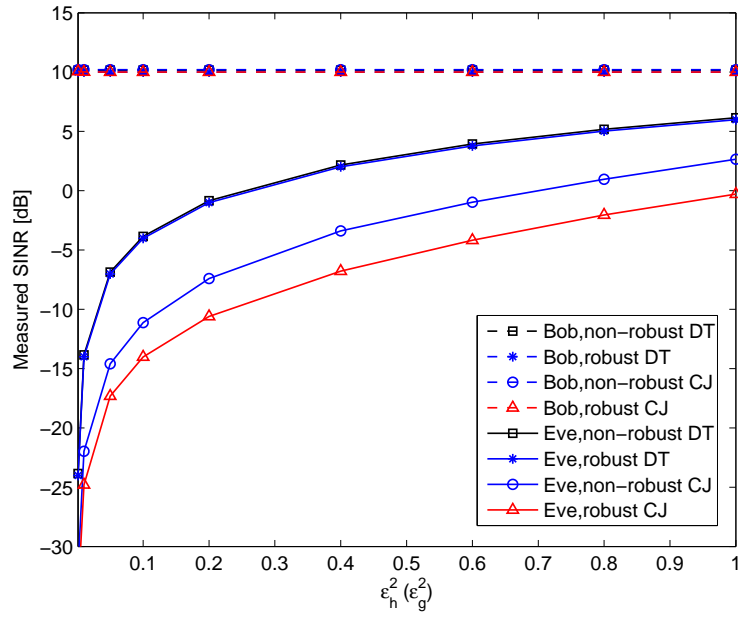Fig. 4. Worst-case secrecy rate vs. SINR constraint at Bob, $\epsilon_h^2 = \epsilon_g^2 = 0.5$, $P = 10$dB.

Fig. 5. Worst-Case secrecy rate vs. channel mismatch, with QoS constraint $\gamma_t = 10$dB, $P = 10$dB.